IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
LYNCHBURG DIVISION

IN THE MATTER OF THE SEARCH OF:

**701 NORWOOD STREET,
LYNCHBURG, VIRGINIA 24504**

Case No. 6:24mj39

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Brandon Smock, a Special Agent ("SA") with Homeland Security Investigations, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant to search the premises located at **701 NORWOOD STREET, LYNCHBURG, VIRGINIA 24504** ("SUBJECT PREMISES"), which is located in the Western District of Virginia, and is further described in Attachment A, for evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. 922(g) and 26 U.S.C. § § 5861, as more specifically described in Attachment B of this affidavit.

2. I am a Special Agent with the U.S. Department of Homeland Security, Homeland Security Investigations ("HSI"), and have been employed by HSI since July 2019. As such, I have attended and graduated the Federal Law Enforcement Training Center Criminal Investigator Training Program as well as the HSI Special Agent training program. Prior to becoming a Special Agent, I was a sworn Police Officer with Prince William County Police Department in Virginia beginning in 2012. In the fall of 2016, I became a Detective assigned to the Special Victims Unit of the Prince William County Police Department Criminal Investigations Division. In that capacity, I investigated various criminal offenses, including physical and sexual assault offenses

against children. In the fall of 2017, I was assigned to the Northern Virginia/District of Columbia Internet Crimes against Children ("ICAC") Task Force. Shortly after, I was sworn in as a Special Police Officer with the Virginia State Police. I was later sworn in as an HSI Task Force Officer. During my time as a Detective, I became a certified Child Forensic Interviewer and became certified in forensic acquisition of digital evidence, Peer-to-Peer data sharing investigations, and undercover chat concepts and techniques. As part of my current duties as an HSI Special Agent, I investigate violations of law relating to the illegal importation and exportation of weapons, technology and other merchandise and contraband into and out of the United States. I have training and experience in the enforcement of the laws of the United States, including the preparation, presentation, and service of subpoenas, affidavits, criminal complaints, search warrants, and arrest warrants. Additionally, I have experience involving investigations, including but not limited to production, distribution and possession of child pornography, distribution of controlled substances, in which I have used various investigative techniques including surveillance, undercover operations, physical searches, and electronic examinations of evidence. Further, through training and experience, I know criminal activity including child exploitation, human trafficking, narcotic and firearm crimes occur via and communicated across various forms of electronic devices. As a federal agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States. I am thus a "federal law enforcement officer" as defined by Fed. R. Crim. P. 41(a)(2)(C).

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. I have set forth only the facts I believe are necessary

to establish probable cause to believe that contraband, evidence and property designed for use, intended for use, or used in committing (i.e., instrumentalities) of violations of Title 18 U.S.C. 922(g) and 26 U.S.C. § § 5861, are presently located at the **SUBJECT PREMISES**.

STATEMENT OF PROBABLE CAUSE

4. On January 8, 2024, United States Magistrate Judge C. Kailani Memmer issued a search warrant for 701 Norwood St., Lynchburg, Virginia 24504, based on probable cause that Les Christopher Burns (BURNS) had imported and was in possession of multiple machine gun conversion devices, or Glock switches. *See* search warrant Case Number 6:24-mj-1.

5. That warrant was executed on January 9, 2024. Inside the residence, agents discovered, among other things, four Glock switches, at least two silencers, a Remington 30-06 rifle, a Beretta pistol, multiple firearm magazines, multiple rounds of ammunition of various calibers, a laptop, and a cellphone. During the execution of the search warrant, an interview was conducted with BURNS regarding the investigation. BURNS stated he would purchase and sell firearm parts to individuals in an attempt to make profit. Additional investigation into BURNS' criminal history revealed that in 1999 BURNS, then a juvenile, was convicted as an adult of Burglary in the Circuit Court of Bedford, Virginia, which is a crime punishable by a term of imprisonment exceeding one year. Further, on October 30, 2023, the Lynchburg, Va. Juvenile and Domestic Relations Court issued a two-year protective order against BURNS, restraining him from contact with his former spouse. BURNS was personally served a copy of this protective order.

6. A subsequent search of the contents of that laptop revealed PDF documents describing how to make explosives, how to make methamphetamine and LSD, how to 3D print a Glock firearm, and how to assemble a Glock firearm. Investigators also discovered multiple Google searches from November 2023 researching the restoration of firearms rights in Virginia.

A subsequent search of a cellphone seized, indicated the device was wiped remotely the day after the device was seized. No data was able to be recovered.

7. As a result of the investigation into BURNS and the items discovered at his residence, on November 14, 2024, a federal grand jury returned a four-count indictment charging BURNS with unlawfully possessing a machine gun (Glock Switch), unlawfully possessing firearms as a prohibited person, and unlawfully possessing firearms in violation of the National Firearms Act all in violation of Title 18 U.S.C. §§ 922(o), (g)(1), (g)(8), and Title 26 U.S.C. §§ 5861(i) and (d). A warrant for his arrest was subsequently issued.

8. On December 10, 2024, your affiant and other agents, went to the **SUBJECT PREMISES** to arrest BURNS. Your affiant knocked on BURNS' front door and he answered wearing a robe. BURNS was advised there was a warrant for his arrest, to which BURNS requested to put on clothes which were located inside his residence. BURNS advised that there were no other occupants inside the residence and indicated his clothes were "right here." Your affiant requested to enter the residence and BURNS led your affiant into the adjacent living room and identified his clothing lying on a piece of furniture in the living room. While BURNS' clothes were being checked for weapons, adjacent to BURNS and your affiant, your affiant observed, in plain view, what your affiant believed to be a lower receiver for a handgun and a firearm magazine sitting on what appeared to be a table. Another agent observed what appeared to be a slide for a handgun located on the same table.

9. After dressing, BURNS was handcuffed and placed in the rear of a Lynchburg Police Department Patrol vehicle and read his *Miranda* warnings. BURNS agreed to speak with your affiant and signed a Department of Homeland Security Statement of Rights waiver. Afterwards, BURNS advised the lower receiver on the table was given to him to fix, but it was

broken. Additionally, BURNS confirmed the presence of the firearm magazine and firearm slide. To your affiant's knowledge, these items were not present during the January search warrant execution of BURNS' residence. Further, BURNS stated that other firearm parts were in a box inside the residence.[1]

10. After transporting BURNS to the United States Marshals Office, your affiant confirmed BURNS resides at his residence alone

11. Based on the foregoing, your affiant asserts that probable cause exists to believe that Les Christopher BURNS has continued to unlawfully possess firearms after having been previously convicted of a crime punishable by imprisonment for a term exceeding one year, and while subject to a protective order, and that there is probable cause to believe that firearms (including those defined in the National Firearms Act as were previously discovered by agents), firearm parts, and related accessories, are located inside his residence, the **SUBJECT PREMISES**.

12. Further, BURNS previously admitted that he purchased and sold firearm parts in attempt to make profit and the previous cell phone seized from the SUBJECT PREMISES was remotely wiped, and your affiant's knowledge that individuals who traffic/import controlled/illicit items often research, identify, purchase, chat/discuss the controlled item via the Internet, and that this information can be recovered by forensic examination of the various computer devices used for these purposes, which can include but is not limited to using handheld cellular telephones, laptop computers, desktop computers, tablets and other personal devices, thus there is probable cause that evidentiary items may be located on or in electronic devices.

---

[1] Burns stated the firearm parts in the box were left by agents after the execution of the previous search warrant. However, your affiant's knowledge, no usable firearm parts were left at the **SUBJECT PREMISES**.

Background on Computers, Digital Devices, and Storage Media

13. I submit that if a computer, digital device, including a wireless cellular telephone, and/or storage media are discovered in the SUBJECT PREMISES, there is probable cause to believe records or communications will be stored on those computers, devices, phones, and storage media for the following reasons

a. Based on my knowledge, training and experience, I know that computer files or remnants of such files can be recovered months or years after they have been downloaded onto a storage medium, deleted or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear, rather that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on storage medium that is not currently being used by an active file – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media – in particular, computers' internal hard drives – contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating systems or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

14. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device(s) because:

15. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the data files were created and the sequence in which they were created.

16. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and duration, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware

detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information descried herein may either inculpate or exculpate the computer user. Finally, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

17. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them and when.

18. The process of identifying the exact electronically stored information on a storage medium necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always something easily reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

19. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

20. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a

computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing in a controlled environment will allow examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under these warrants could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

21. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrants, and would authorize a later review of the media or information consistent with the warrants. The later review may require techniques, including but not limited to computer-assisted

scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

22. Based on all the foregoing information, your affiant respectfully requests the Court issue a search warrant to search the residence located at **701 Norwood Street, Lynchburg, Virginia 24504** (including all outbuildings and curtilage) for the items described in Attachment B.

Respectfully submitted,

BRANDON M SMOC Digitally signed by BRANDON M SMOC
Date: 2024.12.10 18:33:05 -05'00'

Brandon Smock, Special Agent
Homeland Security Investigations

Subscribed and sworn to me by telephone this 10th day of December, 2024.

HON. C. KAILANI MEMMER
UNITED STATES MAGISTRATE JUDGE